STATE OF ALABAMA

Information Technology Procedure

Procedure 600-03P1_Rev B: Security Council

1. INTRODUCTION:

To enhance the level of information security, protect State information and data against internal and external threats, and to ensure compliance with State information security policies, procedures, and standards the Chief Information Officer (CIO) has established the State Information Technology (IT) Security Council. This document identifies Security Council membership and procedures.

2. OBJECTIVE:

Implement requirements of State IT Policy 600-03: Security Council.

3. SCOPE:

This procedure applies to all State of Alabama employees, contractors, vendors, or business partners who are asked to participate as in the State IT Security Council process.

4. PROCEDURES:

4.1 SECURITY COUNCIL MEMBERSHIP

Policy: A council comprised of information technology and security personnel shall be created and convened monthly (or as needed) to discuss relevant information technology and security matters affecting the State. Membership shall be specified in applicable procedures.

Security Council membership shall include individuals serving in the following positions:

- Voting Members:
  - Assistant Director, IT Planning, Standards and Compliance
  - Assistant Director, Infrastructure
  - Assistant Director, ISD Operations
  - Assistant Director, Application Development

Any voting member unable to attend a council meeting must send an alternate to the meeting to vote on their behalf. No voting member may cast more than one vote. In the event of a tie vote, if the matter cannot be resolved by the council then it will be escalated to the CIO for a decision.

- Advisory (non-voting) Members:
  - ISD Information Security Officer - Council Leader
  - ISD Network Operations Manager

- ISD Mainframe Systems Manager
- ISD Systems Administration Manager
- ISD Security Business Partner(s) representatives
- Other personnel when requested to attend
- At-large members (2)

At-large members shall be selected IT Managers, Information Security Officers, or security administrators from agencies other than the Department of Finance/ISD. Two at-large members shall be selected annually by the voting members of the council, and will participate in all council proceedings for 12 consecutive months. At-large members do not vote but are encouraged to send an alternate to the meetings if they cannot attend.

4.2 COUNCIL SCHEDULE

4.2.1 Monthly Meetings

The Security Council will meet monthly, normally on the third Wednesday of each month, for routine business and for emergency sessions at the call of the Council Leader.

4.2.2 Pre-meeting Conference Call

A pre-meeting conference call will be conducted one week prior to the meeting date to verify the items on the agenda and ensure they are ready to be discussed. Council members should review the topics prior to the conference call. Topics will be discussed briefly and if consensus can be reached the item may be closed during the call and removed from the meeting agenda.

4.3 SECURITY EVALUATION REQUEST PROCESS

Policy: The Security Council shall review agencies security needs and plans for deploying information technology resources on the State network or systems, make recommendations to ensure secure implementation of network/system changes, and follow up on the implementation to ensure the required level of security is present to protect State information system resources.

The following illustrates the 4-phased process the Security Council will use to identify issues, gather key information, present data to Council members for review and recommendation, and follow up on the implementation to ensure that approved changes are properly made and the required level of security is present to protect State resources (network and data).

4.3.1 Initiation

Changes to the baseline configuration of the State infrastructure can be initiated by various events or by any entity including customers, application developers, staff, vendor upgrades, or changes to external requirements. All baseline changes must follow a formal change management process, and that process should include the development of a security plan and an evaluation of the security implications as a result of the proposed change.

Security Evaluation Request (SER) – Form 600-03F1: Security Evaluation Request is used to report the analysis findings on any security plan or other issue brought to the Security Council for evaluation and recommendation. The SER form may be assigned to various personnel (including contractors, helpdesk staff, technicians, or managers) for analysis. The SER is logged and tracked as an action item by the Security Council Recorder.

Initiation Phase	
Input:	Identified issue requiring Security Council review Security Plan
Activities:	I1. Issue initiator or requester provides security plan information to Security Council Leader (LDR) I2. LDR forwards info to Security Council Recorder (RCDR) I3. RCDR initiates SER, opens action item, adds item to council agenda, and forwards SER back to LDR I4. LDR assigns SER to Analyst(s); copy RCDR for tracking I5. LDR notifies initiator/requester that issue is being examined
Output:	Partially completed SER Open Action Item

Table 4-1: Initiation

4.3.2 Analysis

Assigned personnel analyze the plan/request, address all security concerns, and prepare a summary of findings and recommendations to present at a designated future council meeting.

Analysis Phase	
Input:	Partially completed SER Security Plan
Activities:	The assigned analyst(s) shall: A1. Review issue/plan/request A2. Collect information A3. Complete SER (reverse) A4. Submit completed SER and all other artifacts to RCDR
Output:	Completed SER and other artifacts

Table 4-2: Analysis

4.3.3 Review

The Security Council reviews the analysis summary and makes the determination whether or not to proceed with the change. If the Security Council determines that the plan/request should be disapproved, a reason is documented on the SER form and feedback is provided to the submitter. If the Security Council does not feel that the change is within their scope, the fully documented SER will be escalated as required for final determination.

Review Phase	
Input:	Completed SER and other artifacts
Activities:	R1. RCDR packages and distributes or posts artifacts for council member review. R2. Council members review artifacts; prepare for discussion and/or decision. R3. LDR initiates meeting request for conference call R4. Briefly discuss issue on conference call. Determine if sufficient info is available to make decision. If so bring to vote, else task for further analysis or defer until meeting for further discussion. R5. RCDR removes from agenda any action items closed during conference call; provides final agenda to LDR. R6. LDR initiates meeting request for monthly council meeting; sends agenda to invitees. R7. Council meets to discuss agenda items and open action items. If no decision is reached, unresolved matters should be escalated as appropriate.
Output:	Council decision or recommendation

Table 4-3: Review

4.3.4 Closure

The Security Council makes the final determination that the implemented change meets all requirements for the security of the State networks and safeguard of data.

Closure Phase	
Input:	Council decision/recommendation
Activities:	C1. LDR notifies initiator/requester of decision or recommendation C2. Implementation actions (may include verification of implementation as directed or recommended, risk assessment, policy changes, additional action items, etc.), as assigned by LDR C3. RCDR documents decision (decision history, lessons learned, etc.) C4. RCDR archives all artifacts C5. RCDR closes action item(s)
Output:	Archived artifacts Closed Action Item(s)

Table 4-4: Closure

4.4 RIGHT TO APPEAL

Agency Heads or IT Managers have the right to appeal if they disagree with the Security Council's decision. All appeals shall be made to the CIO.

5. DEFINITIONS:

SECURITY PLAN: A document identifying the system, the sensitivity of information handled by the system, and system security measures including operational, technical, and management controls, system rules of behavior, risk assessment, and any security awareness and training requirements.

6. ADDITIONAL INFORMATION

6.1 POLICY

Information Technology Policy 600-03: Security Council

6.2 RELATED DOCUMENTS

Form 600-03F1: Security Evaluation Request (SER)

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	06/01/2006	
Rev A	02/06/2007	Added new voting member, AD Operations, and tie-break procedures
Rev B	03/22/2007	Changed at-large membership from 3 months to 1 year.